12 FAM 670

AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY CONTROLS

(CT:DS-215;   09-24-2014)
(Office of origin: DS/SI/CS)

12 FAM 671 PURPOSE

(CT:DS-137;   07-28-2008)

The purpose of this chapter is to provide procedures for implementing AIS security controls required to protect the Department’s automated information systems and the information they process.

12 FAM 672 UNCLASSIFIED FILE TRANSFERS BETWEEN CLASSIFIED, UNCLASSIFIED, AND NON-DEPARTMENT AIS

(CT:DS-182;   11-28-2012)

a. File transfers may not be performed by users without written approval. See 12 FAM 625 and 12 FAM 635 for post and bureau requirements and options for granting approvals.

   NOTE: This section addresses file transfers between systems using physical media (e.g., CD-R or flash/thumb drives); it does not address file transfers between systems performed via an approved system connection, (e.g., e-mail attachments sent or received via the Department’s OpenNet Internet gateway).

b. Systems managers providing a file transfer service are responsible for ensuring that requests are from a legitimate user. Requests should be in writing; clearly identify the file(s) to be transferred; and contain a statement that the user has reviewed the file(s) for content (e.g., to ensure that an unclassified file on a classified system does not have unmarked classified content).

c. If the request is made via other than classified e-mail, the request must be confirmed in one of the following manners:

   (1) The original request may be signed using a Department-issued public key infrastructure (PKI) certificate;

   (2) The requester may send a confirmation of the request via classified e-mail;

(3) The systems manager staff may call the requester at their Department telephone number; or

(4) The requester may speak in person with the systems manager staff.

d. Many of the systems manager responsibilities identified in this section will be carried out by the systems administrator staff. In those instances, the systems manager is responsible for ensuring that there are properly documented procedures in place and that the responsibilities are carried out correctly.

12 FAM 672.1 File Transfer Between a Classified AIS and an Unclassified non-Department AIS

(CT:DS-137; 07-28-2008)

Under no circumstances may an unclassified file be transferred directly between a Department-classified AIS and an Unclassified non-Department AIS. If there is a business requirement to move the file in either direction, it must be done indirectly, via an unclassified Department AIS. The transfer must be accomplished using both the procedure for transferring a file between a classified AIS and an unclassified Department AIS and the procedure for transferring a file between an unclassified non Department AIS and an unclassified Department AIS, in the order appropriate for the transfer (see 12 FAM 672.2 through 12 FAM 672.5).

12 FAM 672.2 File Transfer Downloads from a Classified Department AIS

(CT:DS-182; 11-28-2012)

Only Top Secret-cleared U.S. citizen systems administrator staff, or a user with IRM/IA approval in accordance with 12 FAM 635.2, has the authority to download files (i.e., writing files to removable media) from a classified Department automated information system (AIS) to removable media. Authorized personnel must adhere to the following procedures when downloading files from a classified Department AIS:

(1) Users are only authorized to download data files, (e.g., images, graphic presentations, spreadsheets, text documents) and not executable files;

(2) Use only Department-owned removable media must be used;

(3) The removable media for each transfer must be new or reformatted media;

(4) The removable media must be labeled “SECRET” (for file transfer use only)”;

(5) The removable media must be checked for viruses using the most current virus definitions available immediately when inserted into the classified AIS;

(6) Before transfer, the requestor must perform a full review of each file to be

transferred to identify its content and classification level and ensure proper classification markings are present. The employee performing the transfer should conduct a secondary review for classified markings;

NOTE: If a file previously contained classified data at a higher level than the current marking (e.g., if a user has removed classified information from a document to produce an unclassified version), the systems administrator staff must perform this type of file download to removable media in order to ensure data remnants invisible to the average user are not included in the file transfer;

(7) After the file(s) have been downloaded to the removable media, the employee who performed the transfer must review the removable media to ensure only the files listed for transfer are resident on the media. The media’s Secret label must contain any appropriate handling caveats (e.g. “NOFORN”);

(8) For transfers of unclassified files from a classified Department AIS to an unclassified Department AIS, the removable media used on the classified Department AIS workstation may be placed on an unclassified Department AIS workstation to perform the transfer. The removable media must be immediately checked for viruses using the most current virus definitions available and reviewed again to confirm only the files listed for transfer are resident. The file(s) may then be copied onto the unclassified AIS; *and*

(9) All removable media used in this process on a classified Department AIS must be secured as classified material through final disposition of the media.

12 FAM 672.3 File Transfers from an Unclassified Department AIS to a Classified Department AIS–Unclassified Files Only

(CT:DS-182; 11-28-2012)

Secret-cleared American users domestically and TS cleared systems administrator staff worldwide must adhere to the following procedures when transferring unclassified files from an unclassified Department AIS to a classified Department AIS:

(1) Cleared American systems manager approval in accordance with 12 FAM 635.2 is required for a user to perform a transfer domestically. Users may not transfer files onto a classified AIS overseas;

(2) Users may only transfer data files (e.g., images, slide presentations, spreadsheets, text documents). Users are prohibited from transferring executable files;

(3) The file transfer is only authorized between AIS workstations that have IT-

CCB-approved operating systems configured in accordance with Department security configuration guidelines. These workstations must have the latest anti-virus and definition files installed;

(4) Department-owned, unused, or reformatted nonelectronic digital removable media (e.g., diskette, CD-R), or a dedicated flash drive must be used to perform the file transfer, and the media must be checked for viruses. Reformatted nonelectronic removable media must be labeled "SECRET (for ClassNet-OpenNet file transfer use only)." See 12 FAM 637.1-4 for flash drive requirements;

(5) The files must be copied to the removable media using the operating system file copy command or a utility program approved by the IT-CCB for that purpose. The removable media must be reviewed to confirm that only the files listed to be transferred are resident on the media;

(6) The removable media can then be taken from the unclassified AIS workstation and placed on the classified AIS workstation;

(7) The removable media with files must be virus-scanned to ensure that it is still free of viruses. The removable media must again be reviewed to confirm that only the files listed to be transferred are resident on the removable media. The files may then be copied onto the classified AIS; and

(8) All removable media used in this process must be labeled and secured as classified items until final disposition.

12 FAM 672.4 File Transfers From an Unclassified Non Department AIS to an Unclassified Department AIS–Unclassified Files Only

(CT:DS-182; 11-28-2012)

After receiving the necessary written approval from a supervisor in accordance with 12 FAM 625.2-1, the following procedures must be followed when transferring unclassified files from a non-Department AIS to an unclassified Department AIS:

(1) Only data files (e.g., images, slide presentations, spreadsheets, text documents) may be transferred by users. Executable files are not authorized to be transferred;

(2) The file transfer is only authorized to an unclassified Department AIS workstation that has an Information Technology Change Control Board (IT-CCB)-approved operating system configured in accordance with Department security configuration guidelines. The workstation must have the latest anti-virus and definition files installed;

(3) Only unused or reformatted, nonelectronic removable media (e.g., diskette, CD-R) or a dedicated Department-owned flash drive may be used

to perform the file transfer;

(4) While on the unclassified non-Department AIS, the removable media should be virus scanned to ensure that it is free of viruses and reviewed to confirm that only the file(s) listed to be transferred is/are resident on the removable media;

(5) Upon introduction to the Department AIS, the removable media must be virus scanned again to ensure that it is free of viruses and reviewed to confirm that only the files authorized to be transferred is/are resident on the removable media. (This restriction does not apply to other Department files that may be resident on a flash drive used only with a personally owned and managed secure PC, as defined in the Remote Access and Processing Policy); and

(6) The file(s) may then be copied onto the unclassified Department AIS.

12 FAM 672.5 File Transfers from an Unclassified Department AIS to an Unclassified Non Department AIS–Unclassified Files Only

(CT:DS-137; 07-28-2008)

After receiving the necessary written approval from a supervisor in accordance with 12 FAM 625.2-1, the following procedures must be followed when transferring unclassified files from an unclassified Department AIS to an unclassified non Department AIS:

(1) Only data files (e.g., images, slide presentations, spreadsheets, text documents) may be transferred. Executable files are not authorized to be transferred unless authorized in writing by the Office of Computer Security (DS/SI/CS) and the Office of Information Assurance (IRM/IA);

(2) The file transfer is only authorized from an unclassified Department AIS workstation that has an IT-CCB-approved operating system configured in accordance with Department security guidelines. This workstation must have the latest anti-virus and definition files installed;

(3) Department-owned, -unused, or -reformatted nonelectronic, removable media (e.g., a diskette, CD-R), or a dedicated Department-owned flash drive must be used to perform the file transfer;

(4) The removable media must be virus scanned to ensure that it is free of viruses;

(5) The file(s) must be copied to the removable media using the operating system file copy command or a utility program approved by the IT-CCB for that purpose;

(6) The removable media must be reviewed to confirm that only the file(s) listed to be transferred is/are resident on the media; and

(7) The removable media can then be taken from the unclassified Department AIS workstation and placed on the non Department unclassified AIS.

12 FAM 673 THIN CLIENTS

12 FAM 673.1 Scope

(CT:DS-169; 10-13-2011)

a. Thin clients are subject to the general requirements in 12 FAM 600 and 12 FAH-6 H-540. "Thin clients" are computers with operating systems that run on a remote server and have no removable hard drives (See 12 FAM 090 for a definition of Thin Clients).

b. This policy applies to Department-owned TEMPEST and commercial-off-the-shelf (COTS) thin clients that process classified and/or sensitive but unclassified (SBU) information.

c. Use of thin clients in sensitive compartmented information facilities (SCIFs) also requires Special Security Operations (DS/IS/SSO) approval.

12 FAM 673.2 Thin Client Requirements

(CT:DS-182; 11-28-2012)

a. All thin-client models for use in the Department must reside on the ITCCB baseline approved by the IT Change Control Board. Additionally, the Department's Approved Equipment List (AEL) must list all TEMPEST thin-client models for use in the Department. Posts must install the thin-client model required under their TEMPEST profile as the Department's Certified TEMPEST Technical Authority (CTTA) determines.

b. All thin clients must comply with the Department's Security Configuration Guidelines. Please access the GITM Post Thin Client Admin Guide.

c. All users must log off and power down the thin client at close of business (COB) each day. Users must use the Windows Start Menu—Log Off option and power ON/OFF button to power off the workstation.

d. Users must lock their thin clients when they are away from the workstation. Users must use the "LOCK WORKSTATION" icon on the desktop screen to lock the workstation.

e. Do NOT use CTRL+ALT+DEL on thin clients. Because of the thin client's configuration, users may need to power off and restart in order to log on.

f. Abroad, no classified FLASH thin clients may be installed at lock-and-leave posts. Lock-and-leave posts that currently have FLASH thin clients must ensure that each thin-client device is secured in a GSA-approved security container at COB each day. Additionally, post should advise the Department's

Global Information Technology Modernization program office that their thin clients need replacement with flashless thin clients for the next refresh.

g. Except for 24/7-staffed operations or posts with approval for unattended operations, all classified flashless thin-client image servers must have their hard drives secured in a GSA-approved security container at COB each day. For the purposes of this policy, image servers are local workstations that provide a boot image to flashless thin clients.

h. For TEMPEST thin clients, using external USB ports is prohibited unless the Department's CTTA and IRM/IA authorize it.

i. For COTS-classified thin clients, using external USB ports is prohibited unless IRM/IA authorizes it.

j. System administrators must ensure that DS-approved labels, indicating the highest level of information processed, are affixed to all classified thin clients. RSOs are advised that these devices are NOT considered classified when powered off.

k. Abroad, disposal of thin clients must comply with 12 FAH-6 H-541.5-10, Classified Automated Information Systems (CAIS); 12 FAH-6 H-542.5-10, Unclassified Automated Information Systems (UAIS); and 12 FAH-6 H-633.5-9, Classified Information Processing Equipment (CIPE).

l. Domestically, disposal of TEMPEST thin clients must comply with the National Security Telecommunications and Information Systems Security Advisory Memorandum TEMPEST/1-00, Maintenance and Disposition of TEMPEST Equipment. COTS thin clients must have all memory disposed of by an NSA-approved disintegrator or by sending all memory components via classified pouch or official mail to A/OPR/GSM/SS, as permitted under 14 FAM 732.4, for destruction.

12 FAM 674 UNCLASSIFIED VIDEO TELECONFERENCING

12 FAM 674.1 Scope

(CT:DS-182; 11-28-2012)

a. This policy addresses the minimum security requirements for Department-authorized U.S. Government unclassified video teleconferencing (UVTC) equipment.

b. Using UVTC in Sensitive Compartmented Information Facilities (SCIFs) also requires the Special Security Operations Division (DS/IS/SSO) approval.

12 FAM 674.2 UVTC Requirements

(CT:DS-182; 11-28-2012)

a. To use UVTC equipment , the Office Director, domestically, and the regional security officer (RSO) and information management officer (IMO), abroad, must ensure:

(1) Registration of the UVTC;

(2) Notification of the Video Program Office (IRM/OPS/ITI/SI/DTS) before connecting any equipment to OpenNet; and

(3) Abroad, Inside the CAA, written approval by post's counterintelligence working group (CIWG) and the Countermeasures Program Division (DS/ST/CMP).

b. The IT Change Control Board (IT CCB) must approve all UVTC equipment, and the UVTC setup should maintain a minimum footprint for the camera, speakers, and microphone.

c. When using the UVTC equipment, the user must:

(1) **Face** the UVTC camera away from any classified information; any unrelated Sensitive But Unclassified (SBU) information and Personally Identifiable Information (PII); and any areas outside the UVTC space;

(2) When required, use only IT CCB approved noise-cancelling headsets;

(3) Never **leave** active UVTC sessions unattended;

(4) Log off **when** the UVTC session is completed;

(5) Turn off the UVTC equipment (e.g., camera and microphones) and cover the camera lens when not in use; and

(6) **Abroad, Inside the CAA**, the RSO or PSO and ISSO must ensure UVTC equipment is installed in accordance with 12 FAH-6 H-542.5-5.

d. The system administrator must ensure:

(1) Use of only Department IT CCB-approved UVTC hardware and software (contact the Video Program Office before ordering equipment);

(2) Configuration of UVTC equipment is in accordance with the Department's Video Teleconference Security Configuration Standard, e.g., all auto answering and far end remote control features are disabled. The Standard is available on OpenNet;

(3) Licensing and accessibility for management by the Video Program Office of all OpenNet UVTC equipment; and

(4) Up-to-date maintenance contracts for all OpenNet UVTC equipment in order to ensure that end points on the network have the proper firmware and configuration.

e. The ISSO must ensure UVTC operators receive a copy of the UVTC Cyber Security Awareness briefing which advises the potential risks of using UVTC. See the Cyber Security Awareness Web Site for the latest briefing.

12 FAM 675 SECURE VIDEO TELECONFERENCING (SVTC)

12 FAM 675.1 Scope

(CT:DS-215;   09-24-2014)

a. *This policy addresses the minimum security requirements for Department-authorized Secret collateral and below SVTC equipment used in a SVTC room (e.g., conference room) or outside of a SVTC room (e.g., at the user workstation). See* 12 FAM 674*, Unclassified Video Teleconferencing, for minimum security requirements for Department-authorized unclassified video teleconferencing (*UVTC*) equipment.*

b. *SVTC use inside sensitive compartmented information facilities (SCIFs) requires Special Security Operations Division (DS/IS/SSO) approval.*

12 FAM 675.2 SVTC Requirements

(CT:DS-215;   09-24-2014)

a. *The operation of SVTCs on Top Secret collateral systems is prohibited.*

b. *To use SVTC equipment, the Office Director, domestically, and the Regional Security Officer (RSO), Security Engineering Officer (SEO), and Information Management Officer (IMO), abroad, must:*

   (1) *Domestically, obtain written approval from the Program Applications Division (DS/IS/APD), in coordination with the Facilities Security Division (DS/PSP/FSD);*

   (2) *Abroad, prior to installation, submit a completed SVTC location survey to the Countermeasures Program Division (DS/ST/CMP) and obtain written approval from the post's Counterintelligence Working Group (CIWG) and DS/ST/CMP. (Contact DS/ST/CMP for further guidance on approval requirements.); and*

   (3) *Notify the Video Program Office (VPO) of the Diplomatic Telecommunication Service Program (IRM/OPS/ITI/SI/DTS) before connecting SVTC equipment to ClassNet.*

c. *Abroad, tenant agency-owned SVTC equipment must not be connected to Department systems (See* 12 FAM 635.2*). Tenant agencies that require use of SVTC on ClassNet must contact the VPO.*

d. The use of computerized telephone instruments that could connect to a computer system for SVTC is prohibited.

e. When using the SVTC equipment, the user must:

(1) Direct the SVTC camera so that only the information intended for viewing by conference participants is visible;

(2) Use only Information Technology Configuration Control Board (IT CCB) *approved headsets, microphones, and speakers approved by DS/ST/CMP for the specific SVTC configuration;*

(3) Not leave active SVTC sessions unattended;

(4) Log off when the SVTC session is completed;

(5) Prohibit unauthorized persons from entering the conference room and/or overhearing the conversation while the teleconference is in session; and

(6) Disconnect all SVTC equipment (e.g., cameras, microphones, speakers) from its power supply using a DS approved disconnect switch and cover all camera lenses when not in use.

f. The system administrator must ensure:

(1) Use of only Department-owned and IT CCB-approved SVTC hardware and software (Contact the VPO before ordering equipment for ClassNet);

(2) Notification of the VPO before connecting SVTC equipment to ClassNet;

(3) SVTC equipment complies with the site's TEMPEST requirements;

(4) Configuration of SVTC equipment is in accordance with the Department's Video Teleconference Security Configuration Standard (e.g., all auto answering and far end remote control features are disabled);

(5) ClassNet SVTC equipment licensing and accessibility for management is done by the VPO. For all other classified systems, SVTC equipment licensing and accessibility for management is done by the system owner;

(6) Up-to-date maintenance contracts are in place for all SVTC equipment to ensure endpoints on the network have the proper firmware, configuration, and all maintenance personnel are cleared to the level of the SVTC; and

(7) DS/IS/SSO approval of the installation and use prior to installation of a SVTC within a SCIF.

g. The Information System Security Officer (ISSO) must ensure that individuals initiating SVTC sessions receive a copy of the SVTC Cyber Security Awareness briefing, which advises about the potential risks of using SVTC. See Cyber Security Awareness Briefing for the latest briefing.

12 FAM 676 THROUGH 679 UNASSIGNED